DATA AND CYBER SECURITY

IN PROCUREMENT & SUPPLY CHAIN

MARIE MELIKSETIAN

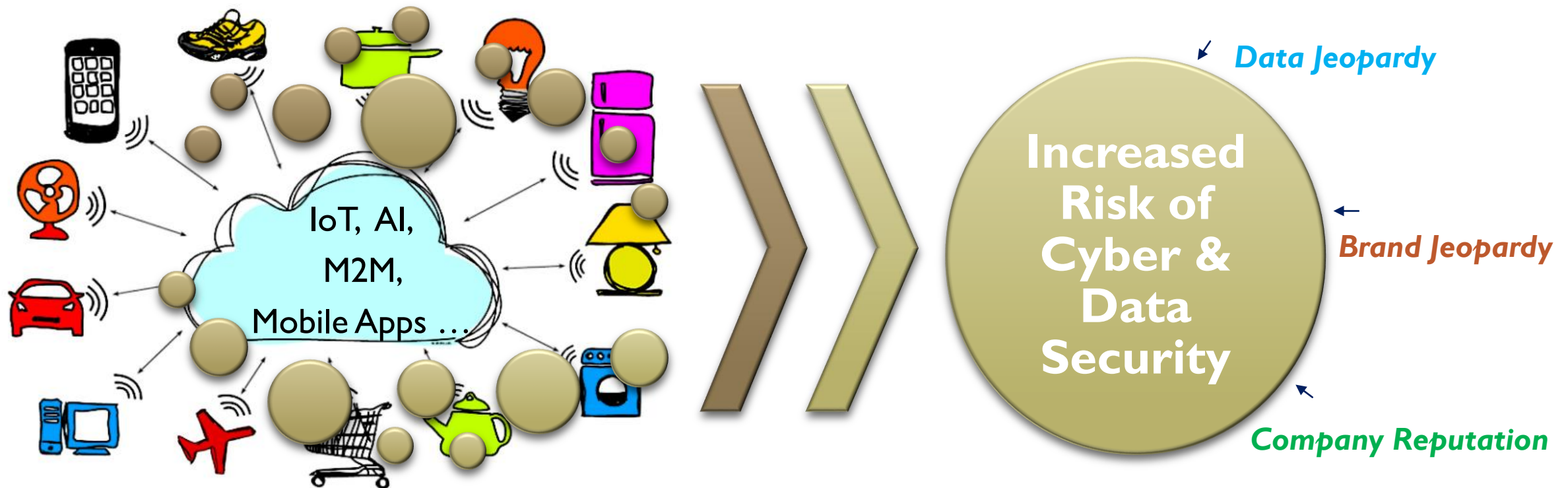**CEO, RELIANCE SOLUTION SERVICES, LLC**

JULY 2018

WHAT ARE WE COVERING TODAY?

- Introduction: Setting the ground

- Role of Procurement and its importance in managing risks

- Issues & Challenges

- Strategies and how to manage the risk

- Conclusion

CYBER AND DATA SECURITY IS EVERYONE'S PROBLEM

Speed of innovation and Technology is Rising. Data complexity is increasing

IoT, AI, M2M, Mobile Apps …

Increased Risk of Cyber & Data Security

Data Jeopardy

Brand Jeopardy

Company Reputation

SOME KEY FACTS

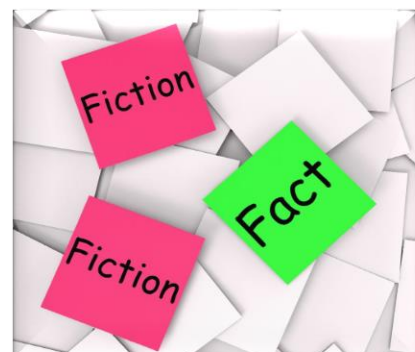**DATA AMOUNT TRAVELLING VIA THE INTERNET**

61,000 GB/sec
By 2020. Compare this to 100 GB/day in the 90's

NOT SIMPLY AN IT ISSUE

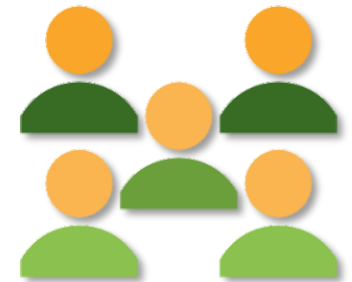Risk is across all business units
Procurement, HR, Finance, Marketing.

MYTH
That you, your company, your business unit will not be effected

IS NO LONGER VALID

CYBER-RISK OVERSIGHT

Only 37% of directors feel their companies are properly secured against cyberattacks *(NACD)*

RISK IN SUPPLY CHAIN

80% of Data Breaches can be tracked back to supply chain

HOW PREPARED ARE YOU?

WHAT IS THE ROLE OF PROCUREMENT

Amongst many roles, of key

- Manage business requirements and life cycle process

- Standardize sourcing requirements

- Identify, select, manage and optimize the supply base

- Negotiate, store, track and manage contracts and commitments

- Develop common processes and manage policies

- Provide technologies for purchasing needs

WHAT DOES PROCUREMENT STRUGGLE WITH

What does procurement struggle with?

- Maverick Spend

- Credibility and usability of data

- Lack of compliance

- Access of Technology

- Stakeholder collaboration

- Access to talent

WHY IS PROCUREMENT CRITICAL TO YOUR SECURITY?

Your most important _Jewels_ are embedded in your operation and cost structure

- Bank accounts

- Financial information

- Customer, government, user information

- Bids, prices, contract information

- Personal information

Critical to managing risk is the maturity of your Procurement

- Data

- Suppliers

- Systems

WHAT ARE SOME OF THE CONCERNS PROCUREMENT WORRIES ABOUT ?

- **Lack of Data Visibility and Control**
  - Data is everywhere
  - Loss of visibility will limit control of data lifecycle

- **Fragmented Tools. Fragmented Data….**
  - Various analytics tools for different needs
  - Data fragmented due to legacy infrastructure
  - Various sources and formats
  - Disruption due to disjointed approach

- **Data Scalability Issues**
  - Data volume and speed from multiple sources
  - Outdated data analytics
  - Holistic view of data requires a scalable solution

- **Visibility to suppliers security processes**
- **Lack of comprehensive Policies**
- **Lack of Governance**
- **Gap and lack of Talent and Skills**

WHAT MUST YOU ASK AND WORRY ABOUT ????

1. How many suppliers providing services to your company are not vetted by Procurement/ IT?
2. What are you doing about it?
3. Have you assessed your core suppliers' cyber security stance?
4. Is it in line with your cyber security requirements and controls?
5. Do you have contract commitments with suppliers protecting you from breach, cyber, data security risks?
6. Do you have policy in place to aggressively eliminate maverick spending and spend creep?
7. If so, are you truly managing it across your organization? And are you getting results?
8. What type of system and data access do your suppliers have?
9. Can they store any of your critical data on their systems?
10. What risks are you exposed to should data/info be accessed through a cyber attack or by competitors?

WHAT MUST YOU ASK AND WORRY ABOUT ????

1. What type of policies do you have in place to manage supplier access risk/security?
2. What type of analytics are you conducting on your spend and suppliers performance?
3. Is one single analytics tool used consistently across your Procurement and organization?
4. If not, what actions are you taking to consolidate formats, sources and tools?
5. Is your Procurement process integrated into a solid data and cyber security solution?
6. Do you have appropriate controls over your data?
7. Are you adhering to certain standards/regulations (i.e., ISO, GDPR)?
8. If not, what actions are you taking?
9. Is your Procurement and Supply Chain team including users trained and re-trained to avoid risks?
10. What is your communication process should a breach take place at a Procurement and Supply Chain level?

WHAT FRAMEWORK SHOULD YOU PUT IN PLACE?

Identify
- **Crown Jewels**
- **Suppliers** not part of your core base and/or with no contracts

Collect
- **Supplier** @ sub-category level by country
- **Contracts** in place by supplier by country

Assess
- Unidentified Suppliers
- Existing Core Suppliers Risks
- Contract Commitments
- Audit results. Actions
- Flow-downs to tier suppliers
- System access. Protocols
- Supplier policies/ processes
- Products, software, infrastructure, operations to protect your jewels
- Emergency/Incidence Support Team

ASSESSMENT INFO

WHAT FRAMEWORK SHOULD YOU PUT IN PLACE?

Develop

- Contract commitments
- Audit/performance review
- Security Policy and control
- Training for Procurement
- Plans/actions in identifying and responding to cyber incidences
- Cross-functional team (Proc. & IT) when assessing/selecting suppliers

Action

- Where/how your critical data will be stored/accessed
- Continuous (24/7/365) 'Reliability tested' support
- Defined timeframe to solution security flaws
- Contractual commitment and legal/financial consequences
- Prove of compliance to security requirements
- Physical security/controls on devices your data is being processed
- Vulnerability history
- Training
- Audit

CONCLUSION

- Procurement and Supply Chain is a critical organization and channel for data and cyber security

- Companies must pay close attention and arm themselves with the necessary support to minimize potential risks

- Financial and reputational risks are at stake and time is of essence.

Time to act!

For additional information contact
Marie Meliksetian
Marie.Meliksetian@RelianceSolutionServices.com
203-512-2035

www.RelianceSolutionServices.com
https://www.linkedin.com/in/marie-meliksetian/